UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/791,019	03/02/2004	Eric Robert Shepherd	QMARK 201.2	1317

90150   7590   05/25/2010
Hoffberg & Associates
10 Bank Street
Suite 460
White Plains, NY 10606

EXAMINER
SHIH, HAOSHIAN

ART UNIT	PAPER NUMBER
2173	

MAIL DATE	DELIVERY MODE
05/25/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Application Number: 10/791,019
Filing Date: March 02, 2004
Appellant(s): SHEPHERD ET AL.

_____

Steven M. Hoffberg
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 02/22/2010 appealing from the Office action

mailed 04/02/2009.

1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of the claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

7,069,586	Winneg et al.	6-2006
2002/0097416	Chang et al.	7-2002

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1-21 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claim 1 recites: "or a normal browser is to be employed" There is no mention in the original specification of employing a normal browser. Further in accordance to the application specification Pub. No. US 2004/0230825 A1, par. [0034], [0035], [0042] and [0048], that a secure browser is deployed **from** a regular/normal browser based on the specified MIME file type that triggers the secure browser. Thus, the limitation includes subject matter that was not described in the original specification.

If the examiner has overlooked the portion of the original specification that describes the

feature of the present invention, then applicant should point it out (by page number and

line number) in the response to this office action.

Applicant may obviate this rejection by canceling the claim.

Claim 9 is rejected similarly as claim 1 above. Further the limitation "insecure browser"

is not mentioned in the original specification.

Claims 2-8 and 10-21 are rejected similarly as set forth above.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form

the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-4 and 6-20 are rejected under 35 U.S.C. 102(e) as being anticipated by

Winneg et al. (Winneg, US 7,069,586 B1).

As to **INDEPENDENT** claim 1, Winneg discloses a secure user interface method, for
interacting with a user through a browser, comprising:

controlling the browser to request a document from a cooperative server (col.8,
lines 57-64; exam-management application allows the user to browse exam documents
from a network address), the browser providing data export support functionality (fig.1,
"116").

receiving data with the browser in response to the request (col.10, lines 5-7);
automatically determining, based on a received data encoding type, whether a secure
browser or a normal browser is to be employed (col.9, lines 45-47, lines 53-55; col.10,
lines 6-13; col.19, lines 62-65; col.26, lines 6-11; a user sends a request to take an
exam by entering a password code, the "exam taking application" determines the
password code maps to the exam file and initiates a secure execution of a secure
browser based on the user request, during the secure browser, unauthorized content
cannot be executed successfully; fig.13, "179", fig.14, "228"; upon the termination of the
secure browser, the system is restored back to its original/non-secure state), the secure
browser having a set of functionality restricted with respect to the normal browser, to
enhance security of a received document against data export (col.15, lines 56-61;
customized template that prevents the user from initiate any external processes);

receiving the secure content for presentation in the secure browser; and
communicating an input from the user, through the secure browser, to a cooperative
server (col.26, lines 6-10; a "password" is required to access the "secure content").

As to claim 2, Winneg discloses the step of limiting access of a user, with the secure browser, to documents outside of a specified set (col.16, lines 50-55; unauthorized contents are disabled from the display).

As to claim 3, Winneg discloses the step of authenticating the secure browser, to assure that the secure browser having the restricted set of functionality is available for presentation of secure content (col.15, lines 63-65; "customized template").

As to claim 4, Winneg discloses the secure browser lacks one or more of the following functions: print, save, cache, cut and copy (col.22, lines 52-59; "prevent the student from copying the information in the buffer to another location).

As to claim 6, Winneg discloses the secure browser restricts termination of execution of the secure browser (col.21, lines 28-33).

As to claim 7, claim 7 incorporates substantially similar subject matter as claimed in claim 6, and is rejected under the same rationale.

As to claim 8, claim 8 is a computer readable media claim of claim 3; it is rejected under similar rationale.

As to **INDEPENDENT** claim 9, claim 9 incorporates substantially similar subject matter as claimed in claim 1, and is rejected under the same rationale.

As to claim 10, Winneg discloses the secure browser provides restricted navigational functionality with respect to the navigational functionality of the insecure browser alone (col.12, lines 46-55).

As to claim 11, claim 11 incorporates substantially similar subject matter as claimed in claim 2, and is rejected under the same rationale.

As to claim 12, Winneg discloses the step of authenticating the secure browser at a remote server prior to presenting the secure content to ensure that the content will only be delivered in the secure browser (fig.8, "146", "158").

As to claim 13, Winneg discloses the secure browser prevents use of the following functions: save, copy, and navigate to unrestricted documents (col.11, 35-39;col.12, lines 52-53; disabling certain user input actions, (e.g., keyboard strokes, mouse clicks) and limiting navigation to only the application window).

As to claim 14, claim 14 incorporates substantially similar subject matter as claimed in claim 6, and is rejected under the same rationale.

As to claim 15, Winneg discloses the secure browser is initiated based on a type

encoding of the received data (col.21, lines 13-15).

As to claim 16, claim 16 incorporates substantially similar subject matter as claimed in

claim 1, and is rejected under the same rationale.

As to claim 17, Winneg discloses the secure browser is granted principal application

level control over graphic user interface inputs from a user (col.12, lines 47-52).

As to claim 18, Winneg discloses the secure browser is granted exclusive control over

graphic user interface functionality when invoked (col.12, lines 47-52).

As to claim 19, Winneg discloses the step of authenticating the server by the secure

browser prior to presenting the secure content (col.8, lines 40; "login").

As to claim 20, claim 20 is a computer readable media claim of claim 6; it is rejected

under similar rationale.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains.
Patentability shall not be negatived by the manner in which the invention was made.

Claims 5 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Winneg in view of Chang et al. (Chang, US 2002/0097416 A1).

As to claims 5 and 21, Winneg does not disclose the secure browser renders text

information as graphic objects.

In the same field of endeavor, Chang discloses renders text information as graphic

objects (fig.1A, 110, 150; "raster"; [0079]).

It would have been obvious to one of ordinary skill in the art, having the teaching of

Winneg and Chang before him at the time the invention was made, to modify the secure

browser interface taught by Winneg to include text conversion taught by Chang with the

motivation being to provide an intended output data format without burdening the user

with the possibility of installing additional drivers/applications/fonts to properly display

the output data (Chang, [0019]).

(10) Response to Argument:

Appellant argues the applied 112 first paragraph against the phrase "or a normal browser is to be employed" (claim 1) and "or whether an insecure browser is to be employed" (claim 9) is improper.

In response to Appellant's argument, There is no mention in the original specification of employing a normal browser or an insecure browser from a browser. As mapped in the summary of claimed subject matter of the appeal brief, pg.3 for claim 1, "or a normal browser is to be employed (Page 13, lines 8-11, Page 11, line 24-page 12, line 7, fig.1: http is a normal browser language, which is used by normal browser until "qmsb" MIME type data is received, which invokes "helper applicaton', the secure browser; Fig.2: Participate runs browser (e.g. IE) normally, until user clicks on link to secure content which triggers call to QSBlaunch.asp, and passes back to IE data with foreign MIME type)".

The citiions on pg.13, line 9-10 "... Launch a secure browser from a normal browser...", and pg.11, line 25-29 "the browser... determining whether a secure browser is required to bem employed" are conncerened with the condition of launching a secure browser from a browser. However, the condition of launching a normal/ insecure browser from a browser is not mentioned.

As mapped in the summary of claimed subject matter of the appeal brief, pg.4 for claim 9, "or whether an insecure browser is to be employed ("Original Browser" in Fig.2)" Fig.2 clear indicates a condition of launching an QSB to process a secure content from a browser and close the QSB and return to the orignal browser. However, the condition of launching a normal/ insecure browser from a browser is not mentioned in the flow diagram.

Furthermore, the applicant's attempt to over come the 112 1st rejection (remarks pg.3-11) are solely directed toward launching a secure browser from a browser when a specified file type is requested from a browser that are not relevant to the previously stated 112 1st rejection.

Appellant argues Winneg does not disclose "automatically determining, based on a received data encoding type, whether a secure browser or a normal browser is to be employed.". that the word "encoding" means, for example:

The way in which symbols are mapped onto bytes, e.g. in the rendering of a particular font, or in the mapping from keyboard input into visual text; A conversion of plain text into a code or cipher form (for decoding by the recipient) en.wiktionary.org/wiki/encoding that Winneg's user passwords is non-overlapping with an "data encoding type" or a "data type encoding".

In response to Appellant's argument, it is common knowledge that data (password

code) inputted in a computer is first encoded/interpreted/mapped onto bytes (0's and

1's) in order for the computer process/understand the inputted data. Winneg discloses

receiving a password code data, matching the received password code data with the

password code data that is encoded as a part of the secure content provided/created by

a content provider (col.10, lines 6-9; col.26, lines 6-11), launching a first application

(col.10, lines 5-10), wherein the first application is a secure browser (col.4, lines 3-6). If

the password code data is incorrect, the secure browser will not launch (col.10, lines 8-

9).

Appellant argues Winneg does not disclose automatically determining, based on

a received data type encoding, whether a secure browser is required to be employed by

a content provider.

In response to Appellant's argument, Winneg discloses matching a correct type of

password code data with the password code data that is associated/encoded with the

secure content provided/created by a content provider (col.10, lines 6-9; col.26, lines 6-

11) to launch a first application (col.10, lines 5-10), wherein the first application is a

secure browser (col.4, lines 3-6).

Appellant argues Winneg does not disclose where the secure browser is initiated

based on a type encoding of the received data.

In response to Appellant's argument, Winneg discloses that a password code is saved/associated with the secure content (col.26, lines 6-11) if a user enters a password code that is the same as a predetermined password that is saved/associated with the secure content, the secure content is then launched on a first application (col.10, lines 5-10), wherein the first application is a secure browser (col.4, lines 3-6).

Appellant argues Winneg does not disclose "the secure browser is initiated based on a code associated with the secure content"

In response to Appellant's argument, Winneg discloses that a password code is saved/associated with the secure content (col.26, lines 6-11) a user that enters a password code that is the same as a predetermined password that is saved/associated with the secure content, the secure content is then launched on a first application (col.10, lines 5-10), wherein the first application is a secure browser (col.4, lines 3-6).

Appellant argues Winneg and Chang do not disclose the secure browser renders text information as graphic objects because Chang only disclose a rasterizer that services all applications on a device.

In response to Appellant's argument, the claimed limitation does not limit the feature of rendering text information as graphic objects to only to the secure browser. Winneg discloses a secure browser (col.4, lines 3-5), Chang discloses converting text object to graphic objects in order to ensure a consistent data display across a plurality of devices wherein a dedicated device or additional software are needed (Chang, [0025]),

It would have been obvious to one of ordinary skill in the art, having the teaching of Winneg and Chang before him at the time the invention was made, to modify the secure browser taught by Winneg to include rendering text objects to graphic objects taught by BBB with the motivation being to provide an intended output data format without burdening the user with the possibility of installing additional drivers/applications/fonts to properly display the output data (Chang, [0019]).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the Above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Haoshian Shih/
Examiner, Art Unit 2173

/Kieu Vu/
Supervisory Patent Examiner, Art Unit 2173

/William L. Bashore/
Supervisory Patent Examiner, Art Unit 2175